REMARKS

Claims 1-14 are in this application. Claim 8 has been canceled. Therefore the rejection of this claim is moot. However, Applicants reserve the right to reintroduce this claim for further prosecution in any future divisional or continuation application. Claims 9-10 have been amended and remain pending in the present application along with unamended claims 1-7 and 11-14.

Claims 8-10 stand rejected under 35 U.S.C. § 101 as allegedly directed toward non-statutory subject matter. Claims 1-14 stand rejected under 35 U.S.C. § 102(e) as anticipated by United States Patent 6,813,357 B1 to Matsuzaki et al ("Matsuzaki"). These rejections are traversed in the following discussion.

35 USC §101 Rejections

Claims 8-10 stand rejected under 35 U.S.C. § 101 as allegedly directed toward non-statutory subject matter. Although Applicants respectfully disagree, claim 8 has been canceled and claims 9-10 have been amended. Accordingly, the rejection of claim 8 is moot. Claim 9 which previously depended upon now-canceled claim 8 has been amended to now depend upon claim 11 which references "[a] recording medium recording a program thereon for controlling a computer…" Claim 10 has been amended to include similar language as claim 11. As the presently pending claims now are implemented in a recording medium, there no longer remains a basis for these rejections.

In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw these rejections.

35 USC §102(e) Rejections

The Examiner rejected claims 1-14 under 35 U.S.C. § 102(e) as being anticipated by Matsuzaki. As a preliminary note, Applicant respectfully notes that a foreign application related to Matsuzaki is discussed in the Background Art section of the application. More specifically, Japanese Patent Application 2000-196581 cited at page 2, line 23 has an application number of JP1998000368817 and is referenced on the face of the cited Matsuzaki patent. Applicants also respectfully bring to the Examiner's attention other disclosed references by Matsuzaki et al that have been previously disclosed: References AH, AI, and AL (disclosed in 10-15-2004 IDS) and Reference AK (disclosed in 1-30-2006 IDS). Relatedly, an IDS identifying two other foreign references by Matsuzaki et al is filed concurrently with this response.

In the present application, the technique described within Matsuzaki is referred to as "a first conventional technique." As discussed in the pending application's specification, the technique used by Matsuzaki (*i.e.* the first conventional technique) is limited because "the modular exponentiation operations cannot be placed in pre-calculation prior to reception of the group key." Specifically, as discussed in the Background Art section (at page 2, line 26 to page 3, line 11), Matsuzaki:

> . . . [E]mploys an algorithm that makes the amount of communication and the amount of time delay after determination of an exclusion-target terminal not proportional to the number "n" of subscribers as a member of the group. When employing the above-described algorithm and assuming that the maximum number of terminals to be excluded is "k," a number, proportional to "k," of modular exponentiation operations have to be performed by each of the subscriber terminals to calculate the group key. Accordingly, if "k" is far smaller than "n" (k << n), key distribution according to this technique can be made far more effectively than a general distribution of group key. For instance, when assuming that a system (n = 10,000) includes 10,000 subscriber terminals and the number of terminals to be excluded is 100 (k = 100), although the general distribution of group key needs processing to be performed a number of times proportional to the number "10,000," key distribution according to the first conventional technique disclosed in the publication needs processing to

> be performed a number of times proportional to the number "100."
>
> However, in a system (e.g., a system for providing services to mobile terminals such as a portable telephone) including up to some million subscriber terminals and in a similar system, it is required to make the number "k" that represents the maximum number of terminals to be excluded enlarged (e.g., some thousands to some ten thousands) to meet the scale of a group. This makes computation load on a terminal that is poor in its computing ability become considerable, which load is imposed by decryption and is proportional to the number "k." Therefore, it is desirable to perform group key distribution that needs decryption to be performed a number of times not proportional to the number "k," or, if possible, a constant number of times.

Anticipation of a claim requires that each and every element of that claim be disclosed in a single prior art reference. *See* Section 2131 of MPEP. Applicants respectfully traverse the anticipation rejection of claim 1 because Matsuzaki fails to disclose "individual key update information corresponding to said specific number of subscriber terminals and used to perform a part of decryption of a second group key, said second group key being updated after a group key is updated, and wherein said specific number of subscriber terminals decrypt said first group key distributed from said key distribution server by use of results obtained by processing operations performed based on said key update information previously obtained and used to decrypt said first group key, as well as by use of said decryption information distributed from said key distribution server."

The Office Action alleges that Matsuzaki discloses this element in column 15 at lines 1-44, which is reproduced in relevant part below:

> (2) It is difficult for the excluded terminal 5 to calculate the common key K and the common data M in the key sharing phase. Information held by the terminal 5 excluded in the key sharing phase are

> exclusive information: C2 (=y^{S5} =g^(kxS5) modp)
> ciphertext: C3 (=MxK=Mxg^(kxS) modp)
>
> in addition to the above (1). These are equal to the ciphertext in the ElGamal cipher. Accordingly, if the moduli p, q and the integer k are set sufficiently large, this ciphertext results in the ElGamal cipher and thus it becomes difficult to calculate the common key K and the common data M based on them. More particularly, it is preferable that p should be set to 1024 bits or more and k, q be set to 160 bits or more.
>
> In the preparatory phase after the key sharing has been completed while excluding the terminal 5, it is possible to exclude the terminal 5 continuously. This is the case that, for example, during when the cipher communication is carried out by five terminals which can share the common secret key in the group, first the terminal 5 is lost or robbed and then four remaining terminals share a new common secret key correspondingly.
>
> Then, if the terminal 4 is also lost or robbed, remaining terminals must share a next common key while excluding both the terminals 4, 5. For this purpose, in the key sharing preparatory phase after the terminal 5 has been excluded, the base station and the terminals 1 to 3 formulate new common data M' (simply an exclusive logical sum of M1 and M2 may be calculated, or a Hash value of a sum of M1 and M2 may be calculated by using the Hash function) based on the common data M1 used in excluding the terminal 5 and the common data M2 used in excluding the terminal 4. According this method, the terminal 5 which cannot obtain the common data M1 and the terminal 4 which cannot obtain the common data M2 cannot formulate the new common data M'. Similarly, the preparatory information, the exclusive information, and the ciphertext, which are used to share the common data M2, may be distributed in secret by using the common data M1. According this method, the terminal 5 which cannot obtain the common data M1 and the terminal 4 cannot obtain the common data M4.
>
> Matsuzaki column 15, lines 5-44

Nowhere in this section of Matsuzaki nor the rest of the Matsuzaki references, however, is the claim element at issue disclosed as there is no disclosure of "individual key update information corresponding to said specific number of subscriber terminals and used to perform ***a part of decryption*** of a second group key, said second group key being updated after a group key is updated, and wherein said specific number of subscriber terminals decrypt said first group key distributed from said key distribution server by use of results obtained by processing operations performed based on said key update information previously obtained and used to decrypt said first group key, as well as by use of said decryption information distributed from said key distribution server" (emphasis added). Because the prior art does not disclose performing "a part of decryption" as claimed, it cannot anticipate claim 1.

Therefore, because Matsuzaki does not disclose each and every element of claim 1, Applicants respectfully request allowance of claim 1. Claims 2-4 should also be allowed at least by virtue of their dependency from claim 1.

Independent claims 5, 7, 10, 11, 12, and 13 each recite an element analogous to the element discussed above in connection with the allowability of claim 1 over the prior art. Matsuzaki does not disclose performing "a part of decryption" as claimed in each of these respective claims. Therefore, Applicant respectfully submits that those claims should be allowed for the same reasons set forth above in support of the allowance of claim 1. Further, Applicants respectfully submit that all dependent claims should be allowed by virtue of their dependency from allowable independent claims.

Conclusion

In view of the above amendments and remarks, Applicants respectfully request reconsideration and the allowance of the pending claims 1-7 and 8-14. An early notification of the allowability of the pending claims is earnestly solicited.

The Examiner is requested to contact the undersigned should there be any questions regarding this communication or if an interview would be helpful in advancing the prosecution of this application.

The Commissioner is hereby authorized to charge any fee(s) necessary to enter this paper and any previous paper, and/or credit any overpayment of fees to deposit account 09-0468.

Respectfully submitted,

/Brian P. Verminski/
Brian P. Verminski
Reg. No. 54,509

IBM CORPORATION
Intellectual Property Law Dept
PO Box 218
Yorktown Heights, NY 10598
Phone: (914)-945-3158